



UNIVERSITEIT • STELLENBOSCH • UNIVERSITY  
jou kennisvenoot • your knowledge partner

# Duality: Windows to the mathematical world

Ingrid Rewitzky

April 2014

# Leonardo da Vinci's perspective

*Perspective is nothing else than seeing a place or objects behind a plane of glass, quite transparent, on the surface of which the objects behind the glass are to be drawn.*

Leonardo da Vinci



Leonardo da Vinci's window

# When you think of computer cables, ...

mental picture of a knot

Photo:



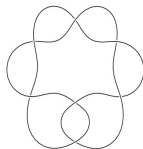
a loop with a number of crossings

Visual:



$$a^2 + a^2z^2 + a^4z^2 + a^6 + a^6z^2a^8$$

Geometric:



## Our perspective

mental or physical

verbal or visual

algebraic or geometric

logical or spatial

What is tightly connected?

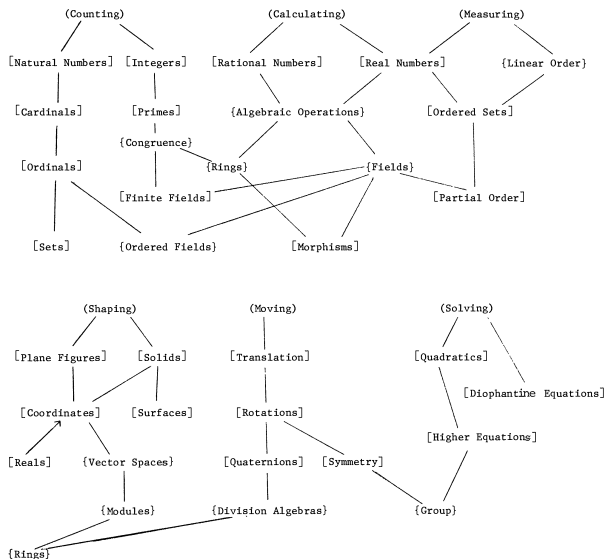
**Equality ?**

# A diversity of mathematical ideas

<b>Human Activity</b>	<b>Mathematical Idea</b>
Counting	to arithmetic and number theory
Measuring	to real numbers, calculus, analysis
Shaping	to geometry, topology
Forming	to symmetry, group theory
Estimating	to probability, measure theory, statistics
Moving	to mechanics, calculus, dynamics
Calculating	to algebra, numerical analysis
Proving	to logic
Puzzling	to combinatorics, number theory
Grouping	to set theory, combinatorics

# Interaction of mathematical ideas

## Origins of Concepts of Abstract Algebra



Everything is a mathematical structure!



# A diversity of mathematical opinions

David Hilbert, Über das Unendliche, Mathematische Annalen (95):  
161-190 (1926) said:

*No one will drive us from the paradise which Cantor created for us.*

Some 'attacked' set theory.

For example, Wittgenstein replied

*If one person can see it as a paradise of mathematicians,  
why should not another see it as a joke?*

# A diversity of mathematical opinions

Others like Mac Lane felt that this

*is a mistakenly one-sided view of mathematics*

and his letter

Mathematical Models: A Sketch for the Philosophy of Mathematics.  
The American Mathematical Monthly, 88 (7) (1981) p 462-472.

may be interpreted as saying that

*In spite of the fundamental achievements of set theory,  
the perfect paradise is still to be found.*

# What is a mathematical structure?

Following the Hilbert program of 1920 and assuming set theory, a structure is a formal axiomatic system consisting of:

Vocabulary: symbols and connectives

Axioms: capturing properties of certain symbols and connectives

Rules: combining symbols and connectives and reasoning about them.

# Not all mathematical structures are first-order theories

A topological space requires the specification of a family of open sets, with no restriction on their cardinalities.

Every reflexive transitive relation gives rise to a topological space, and all finite topological spaces arise in this way.

BUT ...

The number of topologies on a set of infinite cardinality  $\alpha$  is  $2^{2^\alpha}$  whereas the number of first-order structures over a fixed language  $L$  is only  $2^\alpha$  if  $\alpha > |L|$ .

## Some problems with set theory

- ▶ Although set theory allows to define all structures of interest, it does not suggest any general concept of a structure-preserving map.
- ▶ The axioms of set theory are too complicated: on the one hand we all seem to use them every day, and on the other hand only the experts in set theory can properly formulate them.

# What is a mathematical structure?

Following Bourbaki, we start with two finite collections of sets:

Constant sets:  $E, E_1, \dots, E_m$

Variable sets:  $X, X_1, \dots, X_n$

A **scale** is a sequence of sets obtained from the above sets by taking finite products and power sets, and by iterating these operations.

For example,  $\mathcal{P}(\mathcal{P}(X)), \mathcal{P}(X_1 \times X_2 \times X_3), \mathcal{P}(X \times \mathcal{P}(X))$ .

A **type** is a uniformly defined subset  $T(X_1, \dots, X_n)$  of a set in a scale.

For example,

$$T(X) = \{\tau \in \mathcal{P}(\mathcal{P}(X)) \mid \tau \text{ is closed under arbitrary unions and finite intersections}\}$$

A **structure** of a type  $T(X_1, \dots, X_n)$  is an element  $s \in T(X_1, \dots, X_n)$ .

# Isomorphisms

Let  $(X_1, \dots, X_n, s)$  and  $(X'_1, \dots, X'_n, s')$  be mathematical structures of the same type  $T$ . An isomorphism

$$(f_1, \dots, f_n) : (X_1, \dots, X_n, s) \rightarrow (X'_1, \dots, X'_n, s')$$

is a family of bijections  $f_i : X_i \rightarrow X'_i$  ( $i = 1, \dots, n$ ) such that

$$T(f_1, \dots, f_n)(s) = s'.$$



## In general, no structure-preserving maps (homomorphisms)

Let us make now an attempt to define this on all maps – not just bijections.

The most natural way to do so seems to be to use the following two constructions:

- (a) for arbitrary maps  $f_i : X_i \rightarrow X'_i$  ( $i = 1, \dots, n$ ), the induced map  $f_1 \times \dots \times f_n : X_1 \times \dots \times X_n \rightarrow X'_1 \times \dots \times X'_n$  is defined by

$$(f_1 \times \dots \times f_n)(x_1, \dots, x_n) = (f_1(x_1), \dots, f_n(x_n));$$

- (b) for a map  $f : X \rightarrow X'$ , the induced map  $\mathcal{P}(f) : \mathcal{P}(X) \rightarrow \mathcal{P}(X')$  is defined by  $\mathcal{P}(f)(A) = f(A)$ .

Let us apply this to the case of groups, or, more generally magmas, that is, sets equipped with a binary operation with no further assumptions.

We will conclude that a morphism  $f : (X, m) \rightarrow (X', m')$  of magmas is a map  $f : X \rightarrow X'$  with  $f(m) = m'$ , which means that

$$\{(f(x), f(y), f(m(x, y))) \mid x, y \in X\} = \{(x', y', m(x', y')) \mid x', y' \in X'\},$$

and in particular  $f$  must be surjective.

That is, we will get a bad definition . . . .

## Bourbaki morphisms

Let  $T$  be a type, and  $(X_1, \dots, X_n, s)$  and  $(X'_1, \dots, X'_n, s')$  be structures of the same type  $T$ .

A map

$$(f_1, \dots, f_n) : (X_1, \dots, X_n, s) \rightarrow (X'_1, \dots, X'_n, s')$$

is a family of maps  $f_i : X_i \rightarrow X'_i$  ( $i = 1, \dots, n$ ).

A class  $M$  of such maps is said to be a class of morphisms, if it satisfies the following conditions

- (a) If  $(f_1, \dots, f_n) : (X_1, \dots, X_n, s) \rightarrow (X'_1, \dots, X'_n, s')$  and  $(f'_1, \dots, f'_n) : (X'_1, \dots, X'_n, s') \rightarrow (X''_1, \dots, X''_n, s'')$  are in  $M$  then so is  $(f'_1 f_1, \dots, f'_n f_n) : (X_1, \dots, X_n, s) \rightarrow (X''_1, \dots, X''_n, s'')$
- (b) The class of invertible morphisms in  $M$  coincide with the class of isomorphisms.

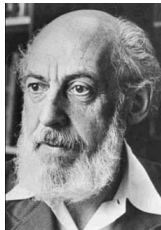
# Category Theory arises naturally

These insights inspired two eminent mathematicians



Saunders Mac Lane  
(1909-2005)

and



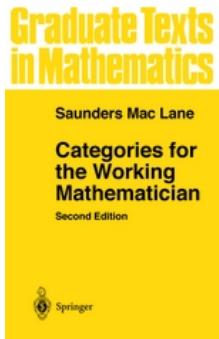
Samuel Eilenberg  
(1913-1998)

to introduce between 1942 and 1945 a modern mathematical framework, called Category Theory, that deals with mathematical structures and structure-preserving maps between them.

# Categories

The **objects** of a category capture a very abstract essence of a structure that is powerful enough to express deep properties of classical mathematical structures and simple enough to justify those properties and to help proving them.

The **morphisms** between objects of a category capture structure-preserving maps between structures.

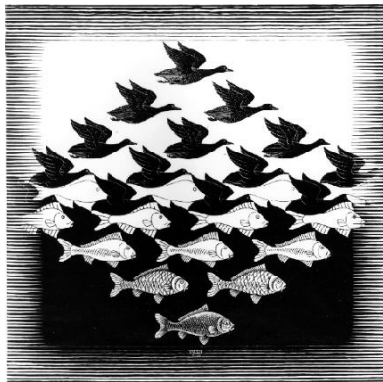


What is tightly connected?

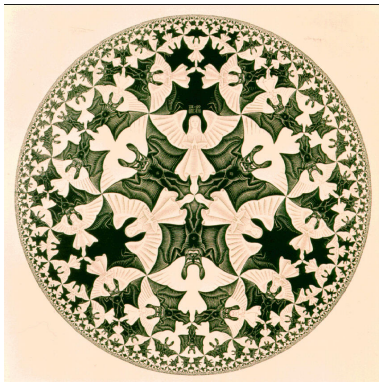
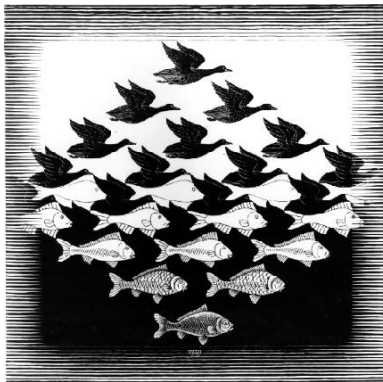
Relate opposites by turning things around ...

**Duality!**

# Escher duality



# Escher duality





# Contravariant duality

The fundamental idea of contravariant duality is:

- ▶ Any entity is determined by its properties.  
This is Leibnitz' principle of the *Identity of Indiscernibles*.
- ▶ Any property is determined by the collection of all entities having that property.  
This is the *Extensionality Principle*.

# Transformations between structures

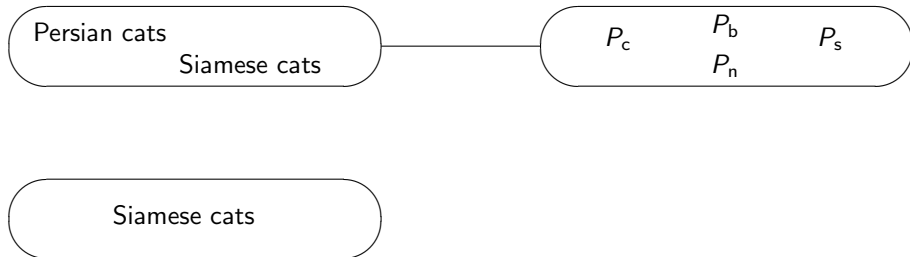
Persian cats

Siamese cats

# Transformations between structures



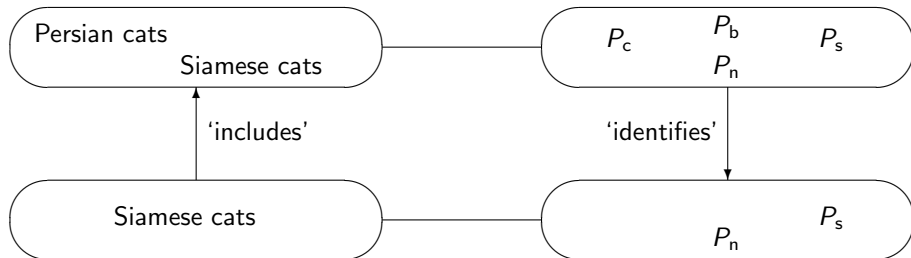
## Transformations between structures



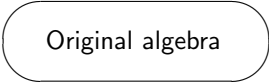
## Transformations between structures



## Transformations between structures



# Transformations between structures



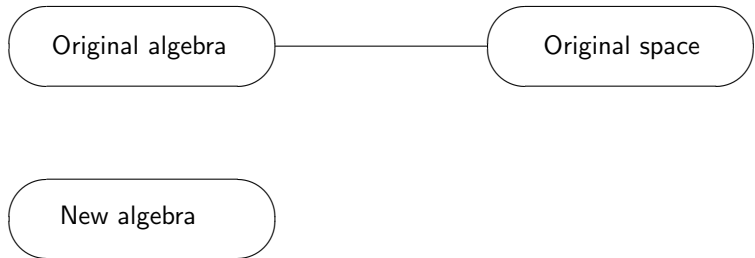
Original algebra

# Transformations between structures

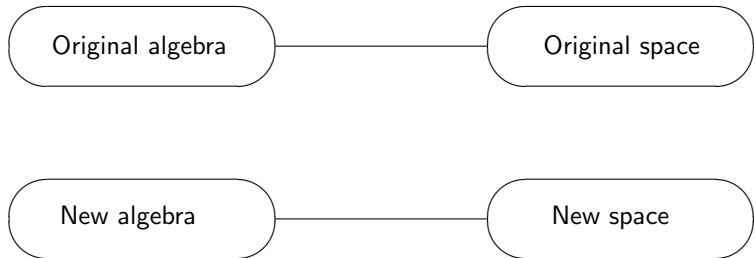




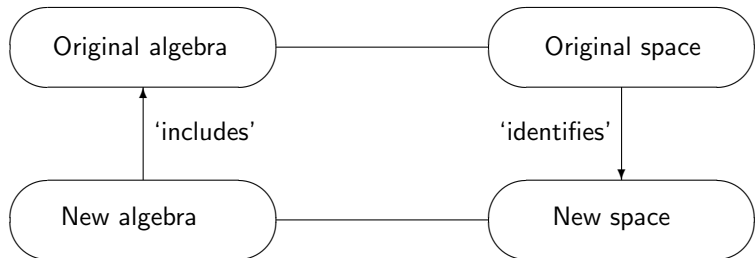
## Transformations between structures



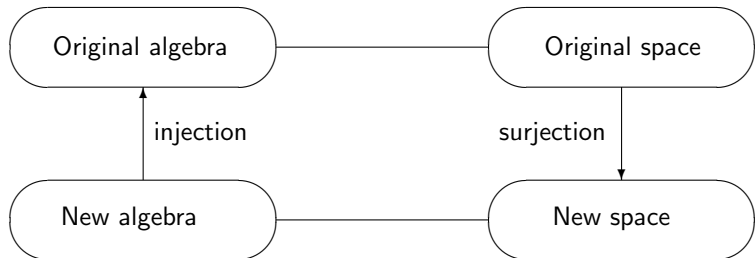
## Transformations between structures



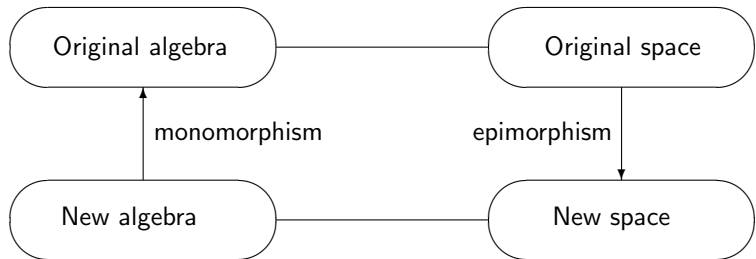
## Transformations between structures



## Transformations between structures



## Transformations between structures



## A challenge

Given a space one can always find an algebra with which to talk about the space.

However, given an algebra, in general, it is not obvious whether there is a space that can be used to talk about the algebra, or whether having such a space would be useful for the algebra.

Marshall Stone (1936, 1937) provided the required insight:

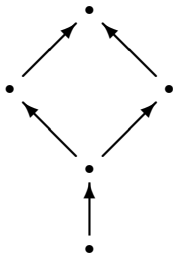
*A cardinal principle of modern mathematical research may be stated as a maxim: "One must always topologize."*

Here 'topologize' means introduce a topology (that is, a collection of sets closed under finite intersections and arbitrary unions).

## **A Hierarchy of Dualities**

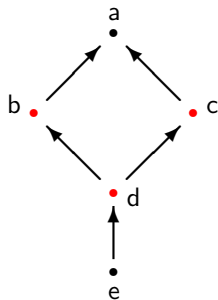


## Birkhoff's duality



Find a suitable structural relationship amongst the **subsets** of the other structure.

## Birkhoff's duality

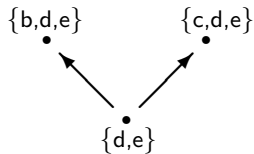
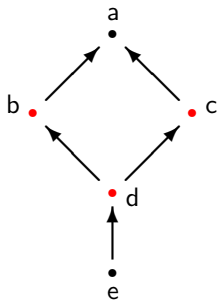


Identify all those objects which have exactly one object below them

— **join-irreducible elements.**

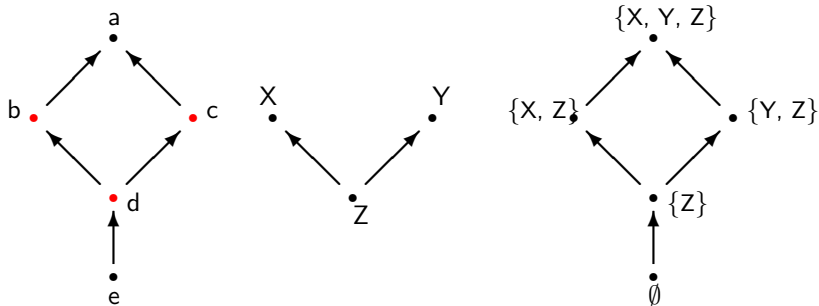
An element  $j \neq 0$  of  $L$  is *join-irreducible* if  $j \leq a \vee b$  implies  $j \leq a$  or  $j \leq b$

# What is duality?



Consider the *downsets* formed from these objects.

# What is duality?



Take downsets.

# Birkhoff's Representation Theorem

Underlying this example is the embedding

$$L \rightarrow \mathcal{P}(\mathcal{J}(L))$$

of a bounded distributive lattice  $L$  in the power set of its join-irreducible elements, defined by

$$a \mapsto \{x \in \mathcal{J}(L) \mid x \leq a\}.$$

The image of this map is completely determined by the order on  $\mathcal{J}(L)$ , namely it is the set  $\mathcal{O}(\mathcal{J}(L))$  of order ideals of  $\mathcal{J}(L)$ .

Any finite distributive lattice can be represented as the lattice of upsets (downsets) of some poset.

# What about infinite distributive lattices?

... there may be **no join-irreducible elements**

For example, in the **lattice of cofinite subsets** of a given infinite set  $S$ , every cofinite set  $A \subseteq S$  may be written as

$$A = (A - \{x\}) \cup (A - \{y\}),$$

for distinct  $x, y \in A$ .

However,

- ▶ in a finite distributive lattice,  
 $\uparrow x$  is a prime filter iff  $x$  is a join-irreducible element.
- ▶ for distributive lattices, in general, the **Prime Filter Theorem** ensures the existence of prime filters.

So **prime filters** will serve as suitable alternative building blocks to join-irreducible elements for bounded distributive lattices.

Consider the mapping

$$L \rightarrow \mathcal{P}(\mathcal{F}(L))$$

of a bounded distributive lattice  $L$  into the power set of its prime filters defined, for any  $a \in L$ , by

$$\phi(a) = \{F \in \mathcal{F}(L) \mid a \in F\}.$$

Then

- ▶  $\phi$  is a lattice homomorphism from  $L$  into  $\mathcal{P}(\mathcal{F}(L))$ ;
- ▶ For each  $a \in L$ ,  $\phi(a) \in \mathcal{U}(\mathcal{F}(L))$ ;
- ▶  $\phi$  is 1-1 (proof requires the Prime Filter Theorem);

But ...

...  $L$  may not be isomorphic to  $\mathcal{U}(\mathcal{F}(L))$ .

Indeed,  $\mathcal{U}(\mathcal{F}(L))$  is always a complete lattice even if  $L$  is not complete.

# Discrete duality for bounded distributive lattices

Bounded distributive lattices:  $(L, \vee, \wedge, 0, 1)$

Distributive lattice frames:  $(X, \leq)$  – non-empty posets

Canonical frame of a bounded distributive lattice  $L$  is  $(\mathcal{F}(L), \subseteq)$

Complex algebra of distributive lattice frame  $X$  is  $(\mathcal{U}(X), \vee^c, \wedge^c, 0^c, 1^c)$   
where

$$\begin{aligned}\mathcal{U}(X) &= \{A \subseteq X \mid A \text{ is upclosed}\} \\ &= \{A \subseteq X \mid [\leq]A = A\}\end{aligned}$$

$$A \vee^c B = A \cup B$$

$$A \wedge^c B = A \cap B$$

$$0^c = \emptyset$$

$$1^c = X$$



# Discrete duality for bounded distributive lattices

Every bounded distributive lattice is embeddable in the complex algebra of its canonical frame.

*Stone mapping  $h : L \rightarrow \mathcal{U}(\mathcal{F}(L))$  defined by*

$$h(a) = \{F \in \mathcal{F}(L) \mid a \in F\}$$

*provides the required embedding.*

Every distributive lattice frame is embeddable into the canonical frame of its complex algebra.

*The mapping  $k : X \rightarrow \mathcal{F}(\mathcal{U}(X))$  defined by*

$$k(x) = \{U \in \mathcal{U}(L) \mid x \in U\}$$

*provides the required embedding.*

This representation can be ...

- ▶ extended by adding operators;
- ▶ generalised by weakening the basis of the algebra;
- ▶ fine-tuned by identifying the  $\hbar$ -image of  $L$  within  $\mathcal{U}(\mathcal{F}(L))$

## Discrete duality for possibility lattices

Possibility lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \vee b) = f(a) \vee f(b) \quad \text{and} \quad f(0) = 0.$$

## Discrete duality for possibility lattices

Possibility lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \vee b) = f(a) \vee f(b) \quad \text{and} \quad f(0) = 0.$$

Possibility frame: partially ordered set  $(X, \leq)$  with a binary relation satisfying

$$(\geq; R; \geq) \subseteq R$$

## Discrete duality for possibility lattices

Possibility lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \vee b) = f(a) \vee f(b) \quad \text{and} \quad f(0) = 0.$$

Possibility frame: partially ordered set  $(X, \leq)$  with a binary relation satisfying

$$(\geq; R; \geq) \subseteq R$$

Canonical frame of a possibility lattice  $(L, f)$  is  $(\mathcal{F}(L), \subseteq, R_f)$  where  $R_f \subseteq \mathcal{F}(L) \times \mathcal{F}(L)$  is defined by

$$FR_f G \quad \text{iff} \quad G \subseteq f^{-1}(F).$$

## Discrete duality for possibility lattices

Possibility lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \vee b) = f(a) \vee f(b) \quad \text{and} \quad f(0) = 0.$$

Possibility frame: partially ordered set  $(X, \leq)$  with a binary relation satisfying

$$(\geq; R; \geq) \subseteq R$$

Canonical frame of a possibility lattice  $(L, f)$  is  $(\mathcal{F}(L), \subseteq, R_f)$  where  $R_f \subseteq \mathcal{F}(L) \times \mathcal{F}(L)$  is defined by

$$FR_f G \quad \text{iff} \quad G \subseteq f^{-1}(F).$$

Complex algebra of a possibility frame  $(X, \leq, R)$  is  $(\mathcal{U}(X), f_R)$  where  $f_R : \mathcal{U}(X) \rightarrow \mathcal{U}(X)$  is defined by

$$f_R(A) = \{x \in X \mid R(x) \cap A \neq \emptyset\}.$$

## Discrete duality for necessity lattices

Necessity lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \wedge b) = f(a) \wedge f(b) \quad \text{and} \quad f(1) = 1.$$

## Discrete duality for necessity lattices

Necessity lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \wedge b) = f(a) \wedge f(b) \quad \text{and} \quad f(1) = 1.$$

Necessity frame: partially ordered set  $(X, \leq)$  with a binary relation satisfying

$$(\leq; R; \leq) \subseteq R$$



## Discrete duality for necessity lattices

Necessity lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \wedge b) = f(a) \wedge f(b) \quad \text{and} \quad f(1) = 1.$$

Necessity frame: partially ordered set  $(X, \leq)$  with a binary relation satisfying

$$(\leq; R; \leq) \subseteq R$$

Canonical frame of a necessity lattice  $(L, f)$  is  $(\mathcal{F}(L), \subseteq, R_f)$  where  $R_f \subseteq \mathcal{F}(L) \times \mathcal{F}(L)$  is defined by

$$FR_fG \quad \text{iff} \quad f^{-1}(F) \subseteq G.$$

## Discrete duality for necessity lattices

Necessity lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \wedge b) = f(a) \wedge f(b) \quad \text{and} \quad f(1) = 1.$$

Necessity frame: partially ordered set  $(X, \leq)$  with a binary relation satisfying

$$(\leq; R; \leq) \subseteq R$$

Canonical frame of a necessity lattice  $(L, f)$  is  $(\mathcal{F}(L), \subseteq, R_f)$  where  $R_f \subseteq \mathcal{F}(L) \times \mathcal{F}(L)$  is defined by

$$FR_f G \quad \text{iff} \quad f^{-1}(F) \subseteq G.$$

Complex algebra of a necessity frame  $(X, \leq, R)$  is  $(\mathcal{U}(X), f_R)$  where  $f_R : \mathcal{U}(X) \rightarrow \mathcal{U}(X)$  is defined by

$$f_R(A) = \{x \in X \mid R(x) \subseteq A\}.$$

## Discrete duality for sufficiency lattices

Sufficiency lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \vee b) = f(a) \wedge f(b) \quad \text{and} \quad f(0) = 1.$$

## Discrete duality for sufficiency lattices

Sufficiency lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \vee b) = f(a) \wedge f(b) \quad \text{and} \quad f(0) = 1.$$

Sufficiency frame: partially ordered set  $(X, \leq)$  with a binary relation satisfying

$$(\leq; R; \geq) \subseteq R$$

## Discrete duality for sufficiency lattices

Sufficiency lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \vee b) = f(a) \wedge f(b) \quad \text{and} \quad f(0) = 1.$$

Sufficiency frame: partially ordered set  $(X, \leq)$  with a binary relation satisfying

$$(\leq; R; \geq) \subseteq R$$

Canonical frame of a sufficiency lattice  $(L, f)$  is  $(\mathcal{F}(L), \subseteq, R_f)$  where  $R_f \subseteq \mathcal{F}(L) \times \mathcal{F}(L)$  is defined by

$$FR_fG \quad \text{iff} \quad f^{-1}(F) \subseteq -G.$$

## Discrete duality for sufficiency lattices

Sufficiency lattice: bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  with a unary operator  $f$  satisfying

$$f(a \vee b) = f(a) \wedge f(b) \quad \text{and} \quad f(0) = 1.$$

Sufficiency frame: partially ordered set  $(X, \leq)$  with a binary relation satisfying

$$(\leq; R; \geq) \subseteq R$$

Canonical frame of a sufficiency lattice  $(L, f)$  is  $(\mathcal{F}(L), \subseteq, R_f)$  where  $R_f \subseteq \mathcal{F}(L) \times \mathcal{F}(L)$  is defined by

$$FR_f G \quad \text{iff} \quad f^{-1}(F) \subseteq -G.$$

Complex algebra of a sufficiency frame  $(X, \leq, R)$  is  $(\mathcal{U}(X), f_R)$  where  $f_R : \mathcal{U}(X) \rightarrow \mathcal{U}(X)$  is defined by

$$f_R(A) = \{x \in X \mid R(x) \subseteq -A\}.$$

## Discrete duality for bounded distributive lattices with operators

Every bounded distributive lattice with operators is embeddable in the complex algebra of its canonical frame.

*Stone mapping*  $h : L \rightarrow \mathcal{U}(\mathcal{F}(L))$  defined by

$$h(a) = \{F \in \mathcal{F}(L) \mid a \in F\}$$

*preserves the unary operator*  $f$ , that is, for any  $a \in L$ ,

$$h(f(a)) = f_{R_f}(h(a)).$$

Every lattice with operator frame is embeddable into the canonical frame of its complex algebra.

*The mapping*  $k : X \rightarrow \mathcal{F}(\mathcal{U}(X))$  defined by

$$k(x) = \{U \in \mathcal{U}(L) \mid x \in U\}$$

*preserves the binary relation*  $R$ , that is, for any  $x, y \in X$ ,  
 $xRy$  iff  $k(x)R_{f_R}k(y)$ .

## Distributive lattice with De Morgan negation

De Morgan lattice: distributive lattice  $(L, \vee, \wedge)$  with greatest element 1 and unary operator  $\neg$  satisfying

$$\neg(a \vee b) = \neg a \wedge \neg b \quad \text{and} \quad a = \neg \neg a$$



## Distributive lattice with De Morgan negation

De Morgan lattice: distributive lattice  $(L, \vee, \wedge)$  with greatest element 1 and unary operator  $\neg$  satisfying

$$\neg(a \vee b) = \neg a \wedge \neg b \quad \text{and} \quad a = \neg \neg a$$

De Morgan frame: partially ordered set  $(X, \leq)$  with  $N : X \rightarrow X$  such that for all  $x, y \in X$ ,

$$x \leq y \Rightarrow N(x) \leq N(y) \quad \text{and} \quad N(N(x)) = x.$$

## Distributive lattice with De Morgan negation

De Morgan lattice: distributive lattice  $(L, \vee, \wedge)$  with greatest element 1 and unary operator  $\neg$  satisfying

$$\neg(a \vee b) = \neg a \wedge \neg b \quad \text{and} \quad a = \neg \neg a$$

De Morgan frame: partially ordered set  $(X, \leq)$  with  $N : X \rightarrow X$  such that for all  $x, y \in X$ ,

$$x \leq y \Rightarrow N(x) \leq N(y) \quad \text{and} \quad N(N(x)) = x.$$

Canonical frame of a De Morgan lattice  $L$  is  $(\mathcal{F}(L), \subseteq, N^c)$  where

$$N^c(F) = L - (\neg F).$$

## Distributive lattice with De Morgan negation

De Morgan lattice: distributive lattice  $(L, \vee, \wedge)$  with greatest element 1 and unary operator  $\neg$  satisfying

$$\neg(a \vee b) = \neg a \wedge \neg b \quad \text{and} \quad a = \neg \neg a$$

De Morgan frame: partially ordered set  $(X, \leq)$  with  $N : X \rightarrow X$  such that for all  $x, y \in X$ ,

$$x \leq y \Rightarrow N(x) \leq N(y) \quad \text{and} \quad N(N(x)) = x.$$

Canonical frame of a De Morgan lattice  $L$  is  $(\mathcal{F}(L), \subseteq, N^c)$  where

$$N^c(F) = L - (\neg F).$$

Complex algebra of De Morgan frame  $X$  is  $\mathcal{U}(X)$  with a unary operator  $\neg^c$  defined by

$$\neg^c A = X - N(A) = \{x \mid N(x) \notin A\}.$$

## Relatively pseudocomplemented lattice

Relatively pseudo-complemented lattice: lattice  $(L, \vee, \wedge)$  with a binary operation  $\rightarrow$  satisfying, for any  $a, b, c \in L$ ,

$$a \wedge c \leq b \quad \text{iff} \quad c \leq a \rightarrow b$$

Note: that any relatively pseudo-complemented lattice is a distributive lattice with greatest element 1 defined by  $a \rightarrow a$ .

## Relatively pseudocomplemented lattice

Relatively pseudo-complemented lattice: lattice  $(L, \vee, \wedge)$  with a binary operation  $\rightarrow$  satisfying, for any  $a, b, c \in L$ ,

$$a \wedge c \leq b \quad \text{iff} \quad c \leq a \rightarrow b$$

Note: that any relatively pseudo-complemented lattice is a distributive lattice with greatest element 1 defined by  $a \rightarrow a$ .

Relatively pseudo-complemented lattice frame: poset  $(X, \leq)$

## Relatively pseudocomplemented lattice

Relatively pseudo-complemented lattice: lattice  $(L, \vee, \wedge)$  with a binary operation  $\rightarrow$  satisfying, for any  $a, b, c \in L$ ,

$$a \wedge c \leq b \quad \text{iff} \quad c \leq a \rightarrow b$$

Note: that any relatively pseudo-complemented lattice is a distributive lattice with greatest element 1 defined by  $a \rightarrow a$ .

Relatively pseudo-complemented lattice frame: poset  $(X, \leq)$

Canonical frame of relatively pseudo-complemented lattice  $L$  is  $(\mathcal{F}(L), \subseteq)$

## Relatively pseudocomplemented lattice

Relatively pseudo-complemented lattice: lattice  $(L, \vee, \wedge)$  with a binary operation  $\rightarrow$  satisfying, for any  $a, b, c \in L$ ,

$$a \wedge c \leq b \quad \text{iff} \quad c \leq a \rightarrow b$$

Note: that any relatively pseudo-complemented lattice is a distributive lattice with greatest element 1 defined by  $a \rightarrow a$ .

Relatively pseudo-complemented lattice frame: poset  $(X, \leq)$

Canonical frame of relatively pseudo-complemented lattice  $L$  is  $(\mathcal{F}(L), \subseteq)$

Complex algebra of relatively pseudo-complemented lattice frame  $X$  is  $(\mathcal{U}(X), \rightarrow_{\leq})$  where, for  $A, B \in \mathcal{U}(X)$ ,

$$A \rightarrow_{\leq} B = [\leq](-A \cup B)$$

# Heyting algebra

Heyting algebra is a relatively pseudo-complemented lattice  $(L, \vee, \wedge, \rightarrow)$  with a unary operation  $\neg$  satisfying, for any  $a, b, c \in L$ ,

$$a \rightarrow \neg b = b \rightarrow \neg a \quad \text{iff} \quad \neg(a \rightarrow a) \rightarrow b = 1.$$

Note: that any Heyting algebra has a smallest element  $0$  defined by  $0 = \neg 1$ .



# Heyting algebra

Heyting algebra is a relatively pseudo-complemented lattice  $(L, \vee, \wedge, \rightarrow)$  with a unary operation  $\neg$  satisfying, for any  $a, b, c \in L$ ,

$$a \rightarrow \neg b = b \rightarrow \neg a \quad \text{iff} \quad \neg(a \rightarrow a) \rightarrow b = 1.$$

Note: that any Heyting algebra has a smallest element  $0$  defined by  $0 = \neg 1$ .

Heyting frame: poset  $(X, \leq)$

# Heyting algebra

Heyting algebra is a relatively pseudo-complemented lattice  $(L, \vee, \wedge, \rightarrow)$  with a unary operation  $\neg$  satisfying, for any  $a, b, c \in L$ ,

$$a \rightarrow \neg b = b \rightarrow \neg a \quad \text{iff} \quad \neg(a \rightarrow a) \rightarrow b = 1.$$

Note: that any Heyting algebra has a smallest element  $0$  defined by  $0 = \neg 1$ .

Heyting frame: poset  $(X, \leq)$

Canonical frame of Heyting algebra  $L$  is  $(\mathcal{F}(L), \subseteq)$

# Heyting algebra

Heyting algebra is a relatively pseudo-complemented lattice  $(L, \vee, \wedge, \rightarrow)$  with a unary operation  $\neg$  satisfying, for any  $a, b, c \in L$ ,

$$a \rightarrow \neg b = b \rightarrow \neg a \quad \text{iff} \quad \neg(a \rightarrow a) \rightarrow b = 1.$$

Note: that any Heyting algebra has a smallest element  $0$  defined by  $0 = \neg 1$ .

Heyting frame: poset  $(X, \leq)$

Canonical frame of Heyting algebra  $L$  is  $(\mathcal{F}(L), \subseteq)$

Complex algebra of Heyting frame  $X$  is  $(\mathcal{U}(X), \rightarrow_{\leq}, \neg_{\leq})$  where, for  $A \in \mathcal{U}(X)$ ,

$$\neg_{\leq}(A) = [\leq](-A)$$

## Boolean lattice

Boolean lattice is a bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  such that for any  $a \in L$  there is an element  $b \in L$  such that

$$a \vee b = 1 \quad \text{iff} \quad a \wedge b = 0.$$

Note that a Boolean algebra is a Boolean lattice in which for each  $a \in L$  there is only one element  $b$  satisfying these conditions.

## Boolean lattice

Boolean lattice is a bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  such that for any  $a \in L$  there is an element  $b \in L$  such that

$$a \vee b = 1 \quad \text{iff} \quad a \wedge b = 0.$$

Note that a Boolean algebra is a Boolean lattice in which for each  $a \in L$  there is only one element  $b$  satisfying these conditions.

Boolean frame: a non-empty set  $X$  – poset with the discrete order

## Boolean lattice

Boolean lattice is a bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  such that for any  $a \in L$  there is an element  $b \in L$  such that

$$a \vee b = 1 \quad \text{iff} \quad a \wedge b = 0.$$

Note that a Boolean algebra is a Boolean lattice in which for each  $a \in L$  there is only one element  $b$  satisfying these conditions.

Boolean frame: a non-empty set  $X$  – poset with the discrete order

Canonical frame of Boolean lattice  $L$  is  $\mathcal{F}(L)$

## Boolean lattice

Boolean lattice is a bounded distributive lattice  $(L, \vee, \wedge, 0, 1)$  such that for any  $a \in L$  there is an element  $b \in L$  such that

$$a \vee b = 1 \quad \text{iff} \quad a \wedge b = 0.$$

Note that a Boolean algebra is a Boolean lattice in which for each  $a \in L$  there is only one element  $b$  satisfying these conditions.

Boolean frame: a non-empty set  $X$  – poset with the discrete order

Canonical frame of Boolean lattice  $L$  is  $\mathcal{F}(L)$

Complex algebra of Boolean frame  $X$  is  $\mathcal{P}(X)$

## Bounded lattices

Bounded (non-distributive) lattices  $(L, \vee, \wedge, 0, 1)$

Doubly-ordered sets  $(X, \leq_1, \leq_2)$  where  $X$  is non-empty and the pre-orders  $\leq_1$  and  $\leq_2$  satisfy , for any  $x, y \in X$ ,

$$x \leq_1 y \text{ and } x \leq_2 y \text{ imply } x = y$$



## Bounded lattices

Bounded (non-distributive) lattices  $(L, \vee, \wedge, 0, 1)$

Doubly-ordered sets  $(X, \leq_1, \leq_2)$  where  $X$  is non-empty and the pre-orders  $\leq_1$  and  $\leq_2$  satisfy , for any  $x, y \in X$ ,

$$x \leq_1 y \text{ and } x \leq_2 y \text{ imply } x = y$$

Canonical frame of bounded lattice  $L$  is  $(\mathcal{X}(L), \subseteq_1, \subseteq_2)$

$$(F, I) \in \mathcal{X}(L)$$

- iff  $F$  is a maximal filter in family of filters disjoint from  $I$   
 $I$  is a maximal ideal in family of ideals disjoint from  $F$   
 $F \cap I = \emptyset$

$$(F_1, I_1) \subseteq_1 (F_2, I_2) \quad \text{iff} \quad F_1 \subseteq F_2$$

$$(F_1, I_1) \subseteq_2 (F_2, I_2) \quad \text{iff} \quad I_1 \subseteq I_2$$

Complex algebra of  $X \in \text{Frm}$  is  $(\mathcal{C}(X), \vee^c, \wedge^c, 0^c, 1^c)$  where

$$\begin{aligned}\mathcal{C}(X) &= \{A \subseteq X \mid lr(A) = A\} \\ A \vee^c B &= l(r(A) \cap r(B)) \\ A \wedge^c B &= A \cap B \\ 0^c &= \emptyset \\ 1^c &= X\end{aligned}$$

where, for  $A \subseteq X$ ,

$$\begin{aligned}l(A) &= \{x \in X \mid \forall y \quad x \leq_1 y \text{ implies } y \notin A\} = [\leq_1](-A) \\ r(A) &= \{x \in X \mid \forall y \quad x \leq_2 y \text{ implies } y \notin A\} = [\leq_2](-A)\end{aligned}$$

# Discrete duality for bounded lattices

Every bounded lattice is embeddable into the complex algebra of its canonical frame.

Define  $h : L \rightarrow \mathcal{C}(\mathcal{X}(L))$  by

$$h(a) = \{(F, I) \in \mathcal{X}(L) : a \in F\}$$

Then

- ▶  $h(a)$  is  $I$ -stable, for each  $a \in L$ .
- ▶  $h$  is a lattice-embedding.

# Observations

Suppose  $(L, \vee, \wedge)$  is a distributive lattice.

Then

- ▶ in  $(X, \leq_1, \leq_2)$   $\leq_2 = \leq_1^{-1}$
- ▶ in the canonical frame  $\mathcal{X}(L)$  the filter-ideal pairs  $(F, I)$  satisfy:
  - ▶  $F$  is a prime filter of  $L$
  - ▶  $I$  is a prime ideal of  $L$
  - ▶  $F = -I$

# Topologising

The embedding

$$L \rightarrow \mathcal{U}(\mathcal{F}(L))$$

of a bounded distributive lattice  $L$  into the lattice of upsets of its prime filters given by

$$a \mapsto \{F \in \mathcal{F}(L) \mid a \in F\}$$

may be characterised by:

- ▶ using set inclusion as a natural **order** on the prime filters, and
- ▶ generating a **topology** on the prime filters using the sets

$$N_a = \{F \in \mathcal{F}(L) \mid a \in F\}, \quad \text{for } a \in L$$

and their complements as a subbasis.

The resulting prime filter space  $(\mathcal{F}(L), \subseteq, \Omega_{\mathcal{F}(L)})$  is a compact totally order disconnected topological space, called a **Priestley space** (or ordered Stone space).

# Topological Representation Theorems

## **Distributive lattices** [Priestley 1972]

- ▶ Every bounded distributive lattice is isomorphic to the lattice of all clopen upsets of some Priestley space.
- ▶ Every Priestley space is order-homeomorphic to the Priestley space of some bounded distributive lattice.

# Topological Representation Theorems

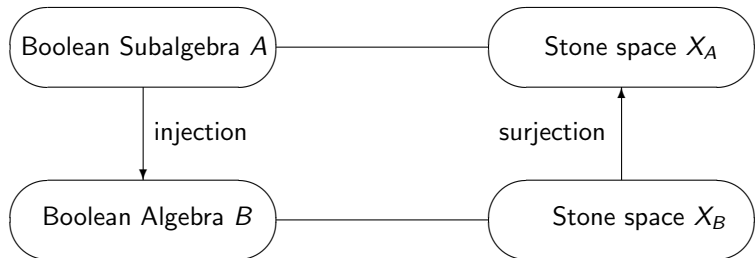
## **Distributive lattices** [Priestley 1972]

- ▶ Every bounded distributive lattice is isomorphic to the lattice of all clopen upsets of some Priestley space.
- ▶ Every Priestley space is order-homeomorphic to the Priestley space of some bounded distributive lattice.

## **Boolean algebras** [Stone 1937]

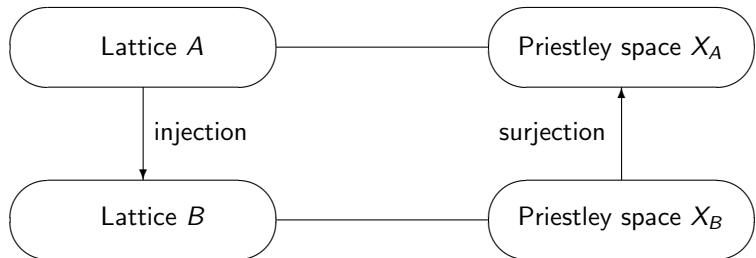
- ▶ Every Boolean algebra is isomorphic to the lattice of all clopen set of some Stone space.
- ▶ Every Stone space is homeomorphic to the Stone space of some Boolean algebra.

## Stone duality for Boolean subalgebras





# Priestley duality for Bounded Distributive Lattices



## **Discrete duality:**

**When algebraic and frame semantics are equivalent**

## Discrete duality

Alg – a class of algebras

Frm – a class of frames

Canonical frames of algebras  $L \in \text{Alg}$

Complex algebras of frames  $X \in \text{Frm}$

$(L, \text{operations})$

$(X, \text{relations})$

$(\mathcal{X}(L), \text{relations}^c)$

$(\mathcal{C}(X), \text{operations}^c)$

# Discrete duality

Alg – a class of algebras

Frm – a class of frames

Canonical frames of algebras  $L \in \text{Alg}$

Complex algebras of frames  $X \in \text{Frm}$

$(L, \text{operations})$

$(X, \text{relations})$

$(\mathcal{X}(L), \text{relations}^c)$

$(\mathcal{C}(X), \text{operations}^c)$

Prove:

- ▶ For every  $L \in \text{Alg}$ , the canonical frame  $\mathcal{X}(L) \in \text{Frm}$ .
- ▶ For every  $X \in \text{Frm}$ , the complex algebra  $\mathcal{C}(X) \in \text{Alg}$ .
- ▶ For every algebra  $L \in \text{Alg}$ ,  $L$  is embeddable into  $\mathcal{C}(\mathcal{X}(L))$ .
- ▶ For each frame  $X \in \text{Frm}$ ,  $X$  is embeddable into  $\mathcal{X}(\mathcal{C}(X))$ .

# Discrete duality

Alg – a class of algebras

Frm – a class of frames

Canonical frames of algebras  $L \in \text{Alg}$

Complex algebras of frames  $X \in \text{Frm}$

$(L, \text{operations})$

$(X, \text{relations})$

$(\mathcal{X}(L), \text{relations}^c)$

$(\mathcal{C}(X), \text{operations}^c)$

Prove:

- ▶ For every  $L \in \text{Alg}$ , the canonical frame  $\mathcal{X}(L) \in \text{Frm}$ .
- ▶ For every  $X \in \text{Frm}$ , the complex algebra  $\mathcal{C}(X) \in \text{Alg}$ .
- ▶ For every algebra  $L \in \text{Alg}$ ,  $L$  is embeddable into  $\mathcal{C}(\mathcal{X}(L))$ .
- ▶ For each frame  $X \in \text{Frm}$ ,  $X$  is embeddable into  $\mathcal{X}(\mathcal{C}(X))$ .

What are the appropriate notions of truth?

# Logical language

Lan - a propositional language built up as follows

Countably infinite set Var of propositional variables.

Formulae are built up from propositional variables using the propositional connectives  $\vee$  and  $\wedge$ .

# Logical language

Lan - a propositional language built up as follows

Countably infinite set Var of propositional variables.

Formulae are built up from propositional variables using the propositional connectives  $\vee$  and  $\wedge$ .

Note:

- ▶ For a bounded distributive lattice we endow the language Lan with propositional constants  $T$  and  $F$ .
- ▶ By a sequent we mean an expression  $\alpha \vdash \beta$  where  $\alpha, \beta$  in Lan.

## Notion of truth determined by Alg

A valuation  $v$  in  $L$  is a function  $v : \text{Var} \rightarrow L$  such that

$$v(\phi \vee \psi) = v(\phi) \vee v(\psi) \qquad v(\phi \wedge \psi) = v(\phi) \wedge v(\psi)$$

A formula  $\alpha$  in  $\text{Lan}$  is true in  $L$  in Alg whenever for every  $v : \text{Var} \rightarrow L$  extended homomorphically to all the formulae of  $\text{Lan}$ ,  $v(\alpha) = 1$  .

A formula  $\alpha$  is Alg-valid (or an Alg-tautology) if  $\alpha$  is true in every algebra from Alg.



## Notion of truth determined by Alg

A valuation  $v$  in  $L$  is a function  $v : \text{Var} \rightarrow L$  such that

$$v(\phi \vee \psi) = v(\phi) \vee v(\psi) \qquad v(\phi \wedge \psi) = v(\phi) \wedge v(\psi)$$

A formula  $\alpha$  in  $\text{Lan}$  is true in  $L$  in Alg whenever for every  $v : \text{Var} \rightarrow L$  extended homomorphically to all the formulae of  $\text{Lan}$ ,  $v(\alpha) = 1$ .

A formula  $\alpha$  is Alg-valid (or an Alg-tautology) if  $\alpha$  is true in every algebra from Alg.

Note:

- ▶ For distributive lattices we define  $v(T) = 1$  and  $v(F) = 0$ .
- ▶ If Alg does not have a designated element 1 or there are no Alg-tautologies in the language, then the notion of truth applies to sequents  $\alpha \vdash \beta$ , where  $\alpha, \beta \in \text{Lan}$ . A sequent  $\alpha \vdash \beta$  is true in algebra  $L$  whenever for every valuation  $v$ ,  $v(\alpha) \leq v(\beta)$ .

## Notion of truth determined by Frm

A model based on a frame  $X$  in  $\text{Frm}$  is a system  $\mathcal{M} = (X, m)$  where  $m : \text{Var} \rightarrow \mathcal{C}(X)$  is a meaning function. If  $X$  is a bounded distributive lattice frame then  $m(T) = X$  and  $m(F) = \emptyset$ .

The satisfaction relation  $\models$  is defined for all formulae  $\alpha, \beta$  of  $\text{Lan}$  by:

$$\begin{aligned} \mathcal{M}, x \models p & \text{ iff } x \in m(p), \text{ for every } p \in \text{Var} \\ \mathcal{M}, x \models \alpha \vee \beta & \text{ iff } \mathcal{M}, x \models \alpha \text{ or } \mathcal{M}, x \models \beta, \\ \mathcal{M}, x \models \alpha \wedge \beta & \text{ iff } \mathcal{M}, x \models \alpha \text{ and } \mathcal{M}, x \models \beta, \end{aligned}$$

Note:

- ▶ If  $\mathcal{M}$  is based on a bounded distributive lattice frame, then  $\mathcal{M}, x \models T$  and  $\mathcal{M}, x \not\models F$ .

## Notion of truth determined by Frm

A formula  $\alpha \in \text{Lan}$  is true in a model  $M$  whenever for every  $x \in X$  we have  $M, x \models \alpha$ .

A formula  $\alpha \in \text{Lan}$  is true in a frame  $(X, R)$  iff  $\alpha$  is true in every model based on this frame.

A formula  $\alpha \in \text{Lan}$  is true in the class Frm of frames iff it is true in every frame  $X \in \text{Frm}$ .

# Notion of truth determined by Frm

A formula  $\alpha \in \text{Lan}$  is true in a model  $M$  whenever for every  $x \in X$  we have  $M, x \models \alpha$ .

A formula  $\alpha \in \text{Lan}$  is true in a frame  $(X, R)$  iff  $\alpha$  is true in every model based on this frame.

A formula  $\alpha \in \text{Lan}$  is true in the class Frm of frames iff it is true in every frame  $X \in \text{Frm}$ .

Note:

- ▶ A sequent  $\alpha \vdash \beta$  is true in  $\mathcal{M}$  whenever  $m(\alpha) \subseteq m(\beta)$ , where  $m(\alpha) = \{x \in X \mid \mathcal{M}, x \models \alpha\}$ .

Assuming that the algebras from Alg are based on lattices with a greatest element, we have:

### **Complex Algebra Theorem**

For every formula  $\phi \in \text{Lan}$  and for every  $X \in \text{Frm}$ , the following conditions are equivalent:

- ▶  $\phi$  is true in all models based on  $X$
- ▶  $\phi$  is true in the complex algebra  $\mathcal{C}(X)$  of  $X$ .

Assuming that the algebras from Alg are based on lattices with a greatest element, we have:

### **Complex Algebra Theorem**

For every formula  $\phi \in \text{Lan}$  and for every  $X \in \text{Frm}$ , the following conditions are equivalent:

- ▶  $\phi$  is true in all models based on  $X$
- ▶  $\phi$  is true in the complex algebra  $\mathcal{C}(X)$  of  $X$ .

### **Duality via truth theorem**

For every formula  $\alpha$  of Lan the following conditions are equivalent:

- ▶  $\alpha$  is true in all algebras  $L \in \text{Alg}$ ,
- ▶  $\alpha$  is true in all models  $(X, m)$ , for  $X \in \text{Frm}$ .

Assuming that the algebras from Alg do not have a greatest element, we have:

### **Complex Algebra Theorem**

For all formulae  $\alpha, \beta$  of Lan and for every  $X \in \text{Frm}$ , the following conditions are equivalent:

- ▶  $\alpha \vdash \beta$  is true in all models based on  $X$
- ▶  $\alpha \vdash \beta$  is true in the complex algebra  $\mathcal{C}(X)$  of  $X$ .

Assuming that the algebras from Alg do not have a greatest element, we have:

### **Complex Algebra Theorem**

For all formulae  $\alpha, \beta$  of Lan and for every  $X \in \text{Frm}$ , the following conditions are equivalent:

- ▶  $\alpha \vdash \beta$  is true in all models based on  $X$
- ▶  $\alpha \vdash \beta$  is true in the complex algebra  $\mathcal{C}(X)$  of  $X$ .

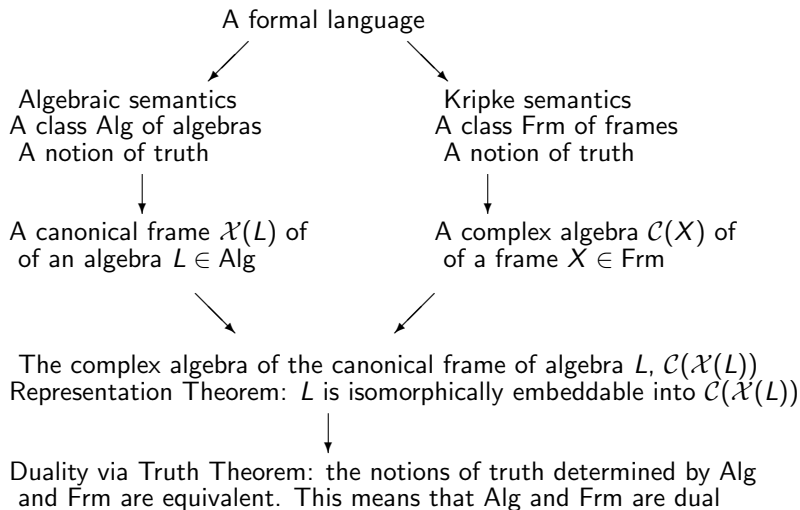
### **Duality via truth theorem**

For all formula  $\alpha, \beta$  of Lan the following conditions are equivalent:

- ▶  $\alpha \vdash \beta$  is true in all algebras  $L \in \text{Alg}$ ,
- ▶  $\alpha \vdash \beta$  is true in all models  $(X, m)$ , for  $X \in \text{Frm}$ .



# A Scheme of Duality via Truth



**Duality: obtaining the 'right window' to a problem**

# Context Algebras, Context Frames, and Their Discrete Duality\*

Ewa Orłowska<sup>1</sup> and Ingrid Rewitzky<sup>2</sup>

<sup>1</sup> National Institute of Telecommunications, Warsaw, Poland

`E.Orłowska@it1.waw.pl`

<sup>2</sup> Department of Mathematical Sciences, University of Stellenbosch, South Africa

`rewitzky@sun.ac.za`

**Abstract.** The data structures dealt with in formal concept analysis are referred to as contexts. In this paper we study contexts within the framework of discrete duality. We show that contexts can be adequately represented by a class of sufficiency algebras called context algebras. On the logical side we define a class of context frames which are the semantic structures for context logic, a lattice-based logic associated with the class of context algebras. We prove a discrete duality between context algebras and context frames, and we develop a Hilbert style axiomatization of context logic and prove its completeness with respect to context frames. Then we prove a duality via truth theorem showing that both context algebras and context frames provide the adequate semantic structures for context logic. We discuss applications of context algebras and context logic to the specification and verification of various problems concerning contexts such as implications (attribute dependencies) in contexts, and derivation of implications from finite sets of implications.

**Keywords:** Duality, duality via truth, representation theorem, formal concept analysis, context, concept, attribute dependency, implication.

## 1 Introduction

A fundamental structure arising in formal concept analysis (FCA) [7,21] is that of a 'context'. In this paper we will consider this notion within the framework of what we refer to as discrete duality. While a classical duality, such as that of, for example, Stone [19] and Priestley [18], includes a representation of a class of algebras in terms of a topological structure, a discrete duality includes a representation for a class of algebras in terms of the relational structures that provide the frame semantics (or equivalently, Kripke-style semantics) of the lattice-based logic associated with the class of algebras. The frame semantics is given in terms of a relational structure without a (non-discrete) topology which

---

\* Ewa Orłowska acknowledges partial support from the Polish Ministry of Science and Higher Education grant N N206 399134, and Ingrid Rewitzky acknowledges partial support from National Research Foundation of South Africa. Both authors acknowledge support from the Poland/SA Bilateral Collaboration Programme.

## Contexts

A formal context is a triple  $(G, M, I)$  where  $G$  and  $M$  are sets and  $I \subseteq G \times M$ .

*Elements of  $G$  are objects.*

*Elements of  $M$  are features.*

*Relation  $I$  is the incidence of the context.*

Central in formal concept analysis is the notion of a *Galois connection* between objects and features.

Algebraically the Galois connection may be captured by two maps  $e$  and  $i$ .

$$i(O) = \{a \in M \mid \forall o \in O, oia\} \quad \text{for } O \subseteq G$$

$$e(A) = \{o \in G \mid \forall a \in A, oia\} \quad \text{for } A \subseteq M.$$

Relationally the Galois connection may be captured by a relation  $R \subseteq G \times M$ .

We formalise this in the notions of context algebra and context frame.

## Context algebra

A *context algebra*  $(L, \vee, \wedge, \neg, 0, 1, e, i)$  is a Boolean algebra  $(L, \vee, \wedge, \neg, 0, 1)$  endowed with two unary operators  $e, i$  satisfying:

- (1)  $\forall a, b \in L, g(a \vee b) = g(a) \wedge g(b)$  for  $g = e, i$
- (2)  $g(0) = 1$  for  $g = e, i$
- (3)  $\forall a \in L, a \leq e(i(a))$
- (4)  $\forall a \in L, a \leq i(e(a))$ .

It follows that the operators  $e$  and  $i$  are antitone and form a Galois connection, that is,

$$a \leq i(b) \quad \text{iff} \quad b \leq e(a), \quad \text{for } a, b \in L.$$

From a complete and atomic context algebra  $\mathcal{A} = (L, \vee, \wedge, \neg, 0, 1, e, i)$  we may define the formal context  $\mathcal{C}_{\mathcal{A}} = (G_{\mathcal{A}}, M_{\mathcal{A}}, I_{\mathcal{A}})$  where, using  $\text{At}(L)$  to denote the set of atoms of  $L$ ,

$$\begin{aligned} G_{\mathcal{A}} &= i[\text{At}(L)] = \cup\{i(\{a\} \mid \{a\} \in \text{At}(L))\} \\ M_{\mathcal{A}} &= e[\text{At}(L)] = \cup\{e(\{a\} \mid \{a\} \in \text{At}(L))\} \\ I_{\mathcal{A}} &= \{(o, a) \mid o \in e(\{a\})\}. \end{aligned}$$

Then

$$e = \llbracket I_{\mathcal{A}} \rrbracket \quad \text{and} \quad i = \llbracket I_{\mathcal{A}}^{-1} \rrbracket,$$

where for  $R \subseteq X \times Y$  and  $Q \subseteq Y$ ,

$$\llbracket R \rrbracket(Q) = \{x \in X \mid Q \subseteq R(x)\}.$$

From a formal context  $\mathcal{C} = (G, M, I)$  we may define a complete and atomic context algebra  $(L_{\mathcal{C}}, i_{\mathcal{C}}, e_{\mathcal{C}})$  where

$$\begin{aligned}L_{\mathcal{C}} &= 2^{G \cup M} \\e_{\mathcal{C}} &= \llbracket I \rrbracket \\i_{\mathcal{C}} &= \llbracket I^{-1} \rrbracket,\end{aligned}$$

where for any  $A \in L_{\mathcal{C}}$  and  $T = I, I^{-1}$ ,

$$\llbracket T \rrbracket(A) = \{x \in G \cup M \mid \forall y, y \in A \Rightarrow xTy\}.$$

Then

$$e = e_{\mathcal{C}} \quad \text{and} \quad i = i_{\mathcal{C}}.$$

## Context frame

A *context frame*  $\mathcal{C} = (X, R, S)$  is a non-empty set  $X$  endowed with binary relations  $R$  and  $S$  such that  $S = R^{-1}$ .

From a context frame  $\mathcal{F} = (X, R, S)$  we may define the formal context  $\mathcal{C}_{\mathcal{F}} = (G_{\mathcal{F}}, M_{\mathcal{F}}, I_{\mathcal{F}})$  where

$$G_{\mathcal{F}} = \text{dom}(R)$$

$$M_{\mathcal{F}} = \text{ran}(R)$$

$$I_{\mathcal{F}} = R.$$

Then

$$\llbracket R \rrbracket = e_{\mathcal{F}} \quad \text{and} \quad \llbracket S \rrbracket = i_{\mathcal{F}}.$$



From a formal context  $\mathcal{C} = (G, M, I)$  we may define a context frame  $(X_{\mathcal{C}}, R_{\mathcal{C}}, S_{\mathcal{C}})$  where

$$X_{\mathcal{C}} = G \cup M$$

$$R_{\mathcal{C}} = I$$

$$S_{\mathcal{C}} = I^{-1}.$$

Then

$$e = \llbracket R_{\mathcal{C}} \rrbracket \quad \text{and} \quad i = \llbracket S_{\mathcal{C}} \rrbracket.$$

## 'Cancellations'

- ▶ If a context  $\mathcal{C} = (G, M, I)$  satisfies  $G = \text{dom}(I)$  and  $M = \text{ran}(I)$ , then  $\mathcal{C} = \mathcal{C}_{\mathcal{A}_{\mathcal{C}}}$ .
- ▶ If a context algebra  $\mathcal{A} = (L, \vee, \wedge, \neg, 0, 1, e, i)$  is complete and atomic, then  $\mathcal{A} = \mathcal{A}_{\mathcal{C}_{\mathcal{A}}}$ .
- ▶ If a context  $\mathcal{C} = (G, M, I)$  satisfies  $G = \text{dom}(I)$  and  $M = \text{ran}(I)$ , then  $\mathcal{C} = \mathcal{C}_{\mathcal{F}_{\mathcal{C}}}$ .
- ▶ If a context frame  $\mathcal{F} = (X, R, S)$  satisfies  $X = \text{dom}(R) \cup \text{ran}(R)$ , then  $\mathcal{F} = \mathcal{F}_{\mathcal{C}_{\mathcal{F}}}$ .

## Canonical frame and complex algebra

Canonical frame of a context algebra  $(L, \vee, \wedge, \neg, 0, 1, e, i) \in \text{Alg}$  is the relational structure  $(\mathcal{X}(L), R^c, S^c)$ , where  $\mathcal{X}(L)$  is the family of prime filters of  $L$ , and for any  $F, G \in \mathcal{X}(L)$ ,

$$FR^cG \quad \text{iff} \quad e(G) \cap F \neq \emptyset \quad \text{and} \quad FS^cG \quad \text{iff} \quad i(G) \cap F \neq \emptyset.$$

## Canonical frame and complex algebra

Canonical frame of a context algebra  $(L, \vee, \wedge, \neg, 0, 1, e, i) \in \text{Alg}$  is the relational structure  $(\mathcal{X}(L), R^c, S^c)$ , where  $\mathcal{X}(L)$  is the family of prime filters of  $L$ , and for any  $F, G \in \mathcal{X}(L)$ ,

$$FR^cG \quad \text{iff} \quad e(G) \cap F \neq \emptyset \quad \text{and} \quad FS^cG \quad \text{iff} \quad i(G) \cap F \neq \emptyset.$$

Complex algebra of a context frame  $(X, R, S) \in \text{Frm}$  is the powerset Boolean algebra with sufficiency operators  $(\mathcal{C}(X), e^c, i^c)$ , where

$$\mathcal{C}(X) = 2^X,$$

$e^c : \mathcal{C}(X) \rightarrow \mathcal{C}(X)$  is defined by

$$e^c(A) = \{x \in X \mid A \subseteq R(x)\} \quad \text{for } A \subseteq X,$$

and  $i^c : \mathcal{C}(X) \rightarrow \mathcal{C}(X)$  is defined by

$$i^c(A) = \{x \in X \mid A \subseteq S(x)\} \quad \text{for } A \subseteq X.$$

## Preservation properties

- ▶ The mapping  $h : L \rightarrow \mathcal{C}(\mathcal{X}(L))$  defined, for any  $a \in L$ , by

$$h(a) = \{F \in \mathcal{X}(L) \mid a \in F\}$$

preserves the operators  $e$  and  $i$ , that is, for all  $a \in L$ ,

$$h(e(a)) = e^c(h(a)) \quad \text{and} \quad h(i(a)) = i^c(h(a)).$$

## Preservation properties

- ▶ The mapping  $h : L \rightarrow \mathcal{C}(\mathcal{X}(L))$  defined, for any  $a \in L$ , by

$$h(a) = \{F \in \mathcal{X}(L) \mid a \in F\}$$

preserves the operators  $e$  and  $i$ , that is, for all  $a \in L$ ,

$$h(e(a)) = e^c(h(a)) \quad \text{and} \quad h(i(a)) = i^c(h(a)).$$

- ▶ The mapping  $k : X \rightarrow \mathcal{X}(\mathcal{C}(X))$  defined, for any  $x \in X$ , by

$$k(x) = \{A \in \mathcal{C}(X) \mid x \in A\}$$

preserves the relations  $R$  and  $S$  in the sense that, for all  $x, y \in X$ ,

$$xRy \text{ iff } k(x)R^ck(y) \quad \text{and} \quad xSy \text{ iff } k(x)S^ck(y).$$

## A discrete duality for contexts

- ▶ The complex algebra of a context frame is a context algebra.
- ▶ The canonical frame of a context algebra is a context frame.
- ▶ Any context algebra  $(L, \vee, \wedge, \neg, 0, 1, e, i)$  is lattice-embeddable into the complex algebra of its canonical frame.
- ▶ Any context frame  $(X, R, S)$  is order-embeddable into the canonical frame of its complex algebra.

## Involutions on Relational Program Calculi

I. M. Rewitzky<sup>1</sup> and J. W. Sanders<sup>2</sup>

### Abstract

The standard Galois connection between the relational and predicate-transformer models of sequential programming (defined in terms of weakest precondition) confers a certain similarity between them. This paper investigates the extent to which the important involution on transformers (which, for instance, interchanges demonic and angelic nondeterminism, and reduces the two kinds of simulation in the relational model to one kind in the transformer model) carries over to relations. It is shown that no exact analogue exists; that the two complement-based involutions are too weak to be of much use; but that the translation to relations of transformer involution under the Galois connection is *just* strong enough to support Boolean-algebra-style reasoning, a claim that is substantiated by proving properties of deterministic computations. Throughout, the setting is that of the guarded-command language augmented by the usual specification commands; and where possible algebraic reasoning is used in place of the more conventional semantic reasoning.

### 1 Introduction

We adopt the familiar view that a semantic model for programming, and for the development of programs from specifications through designs to code, consists of a partially-ordered space. The elements of the space are designs expressed in code—'programs'—and designs (including specifications)

---

<sup>1</sup>Department of Mathematical Sciences, University of Stellenbosch, Stellenbosch, South Africa. Email: [rewitzky@sun.ac.za](mailto:rewitzky@sun.ac.za)

<sup>2</sup>International Institute for Software Technology, United Nations University, Macao. Email: [jeff@iist.unu.edu](mailto:jeff@iist.unu.edu)



# Duality and Involutions

Let  $(B, \vee, \wedge, \neg, 0, 1)$  be a Boolean algebra.

For any function  $f : B \rightarrow B$ , its dual is defined, for any  $a \in B$ , by

$$f^*(a) = \neg f(\neg a).$$

This operator  $*$  on functions over a Boolean algebra is an involution, that is,

$$f^{**} = f.$$

Is there also an involution operator on binary relations?

**NO!**

Let  $\mathcal{R}(X, Y)$  be family of binary relations  $r \subseteq X \times Y$ .

**Theorem** There is no function  $*$  on  $\mathcal{R}(X, Y)$  that is an involution, obeys either of the De Morgan laws and distributes over sequential composition, that is,

- (a)  $\forall r \in \mathcal{R}(X, Y), r^{**} = r$
- (b) either,  $\forall r, s \in \mathcal{R}(X, Y), (r \cap s)^* = r^* \cup s^*$   
or  $\forall r, s \in \mathcal{R}(X, Y), (r \cup s)^* = r^* \cap s^*$ .
- (c)  $\forall r, s \in \mathcal{R}(X, Y), (r; s)^* = r^*; s^*$ .

**Proof:** We argue by contradiction, establishing an untenable identity.

From assumptions (a) and (b) we may establish equivalence of two De Morgan laws in (b), that is,

$$(d) \quad (r \cup s)^* = r^* \cap s^* \quad \equiv \quad (r \cap s)^* = r^* \cup s^*.$$

Assume first De Morgan law holds. Then

$$(r \cup s)^* = (r^{**} \cup s^{**}) = (r^* \cap s^*)^{**} = r^* \cap s^*.$$

Similarly, if second De Morgan law holds.

Now, for all  $r, s, t \in \mathcal{R}(X, Y)$ ,

$$r; (s \cup t) = r; s \cup r; t$$

$$(s \cup t); r = s; r \cup t; r$$

$$r; (s \cap t) \subseteq r; s \cap r; t$$

The reverse inclusion of the last property holds if  $r$  is a function.

However, assuming (a), (b) and (c) we have

$$\begin{aligned}r;(s \cap t) &= (r;(s \cap t))^{**} \text{ by (a)} \\ &= (r^*; (s \cap t)^*)^* \text{ by (c)} \\ &= (r^*; (s^* \cup t^*))^* \text{ by (b)} \\ &= (r^*; s^* \cup r^*; t^*)^* \\ &= (r^*; s^*)^* \cap (r^*; t^*)^* \text{ by (b)} \\ &= (r; s)^{**} \cap (r; t)^{**} \text{ by (c)} \\ &= r; s \cap r; t \text{ by (a)}.\end{aligned}$$

Thus

$$r;(s \cap t) = r; s \cap r; t$$

**A contradiction!**

## A Galois connection

Algebra  $(\mathcal{T}(X), \leq)$  of monotone maps  $f : 2^X \rightarrow 2^X$  where, for any  $f, g \in \mathcal{T}(X)$ ,

$$f \leq g \quad \text{iff} \quad \forall Q \in 2^X, f(Q) \subseteq g(Q).$$

Algebra  $(\mathcal{R}(X), \subseteq)$  of binary relations  $r \subseteq X \times X$ .

## A Galois connection

Algebra  $(\mathcal{T}(X), \leq)$  of monotone maps  $f : 2^X \rightarrow 2^X$  where, for any  $f, g \in \mathcal{T}(X)$ ,

$$f \leq g \quad \text{iff} \quad \forall Q \in 2^X, f(Q) \subseteq g(Q).$$

Algebra  $(\mathcal{R}(X), \subseteq)$  of binary relations  $r \subseteq X \times X$ .

For any  $r \in \mathcal{R}(X)$  we may define a map  $f_r \in \mathcal{T}(X)$  by

$$f_r = [r].$$

For any  $f \in \mathcal{T}(X)$  we may define a relation  $r_f \in \mathcal{R}(X)$  by

$$x r_f y \quad \text{iff} \quad \forall Q \in 2^X, x \in f(Q) \Rightarrow y \in Q.$$

Two sufficiency operators:

$$f_{(-)} : (\mathcal{R}(X), \subseteq) \rightarrow (\mathcal{T}(X), \leq)$$

and

$$r_{(-)} : (\mathcal{T}(X), \leq) \rightarrow (\mathcal{R}(X), \subseteq)$$

with the property that

$$f \leq f_r \quad \text{iff} \quad r \subseteq r_f,$$

or equivalently,

$$f \leq f_{r_f} \quad \text{and} \quad r \subseteq r_{f_r}.$$

Thus

$$((\mathcal{R}(X), \subseteq), f_{(-)}, R_{(-)}, (\mathcal{T}(X), \leq))$$

is a Galois pair.

## A solution!

Given  $r \in \mathcal{R}(X)$ , define  $r^+ \in \mathcal{R}(X)$  by

$$r^+ = r_{[r]^*} = r_{\langle r \rangle}$$

Then  $r^{++} = r_{\langle r_{\langle r \rangle} \rangle}$



## A solution!

Given  $r \in \mathcal{R}(X)$ , define  $r^+ \in \mathcal{R}(X)$  by

$$r^+ = r[r]^* = r\langle r \rangle$$

Then  $r^{++} = r\langle r\langle r \rangle \rangle$

Properties:

- ▶  $r \subseteq s$  implies  $r^+ \supseteq s^+$
- ▶  $r \subseteq r^{++}$
- ▶  $r \subseteq s^+$  iff  $s \subseteq r^+$
- ▶  $(r \cup s)^+ = r^+ \cap s^+$
- ▶  $(r \cap s)^+ \supseteq r^+ \cup s^+$
- ▶  $(r; s)^+ = r^+; s^+$
- ▶  $\emptyset^+ = X \times X$
- ▶  $(X \times X)^+ = \emptyset$

**Duality: potentially the 'right window' to further problem**

## Concluding remark

*It is characteristic of the most successful theories, in mathematics as well as in natural sciences, that they can be presented in several apparently independent ways, which are in a useful sense provably equivalent.*

Sir C.A.R. Hoare, 1995.

## Concluding remark

*A mathematical structure is nothing else than seeing an activity or an entity or a theory through a window to the mathematical world, with duality providing a tight connection between these windows.*

